Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (canceled).

Claim 2. (New) A method of providing a secure network packet, said method comprising:

generating a working key;

encrypting, based at least in part on said working key, target data;

binding together a plurality of key splits to form a cryptographic key;

encrypting, based at least in part on the cryptographic key, said working key; and

forming the secure network packet including the encrypted target data and the encrypted working key;

wherein said plurality of key splits includes a domain key split and a user key split.

Claim 3. (New) The method of claim 2, wherein the working key is generated randomly or pseudo-randomly.

Claim 4. (New) The method of claim 2, wherein the secure network packet is provided at least in part by an integrated circuit.

Claim 5. (New) The method of claim 2, wherein the secure network packet is provided at least in part by a network interface device.

Claim 6. (New) The secure network packet provided by the method of claim 2.

Claim 7. (New) The method of claim 2, further comprising extracting at least one of said plurality of key splits from a credential store.

Claim 8. (New) The method of claim 2, wherein at least one of said plurality of key splits is a default key split.

Claim 9. (New) The method of claim 2, wherein at least one of said plurality of key splits is selected by a user.

Claim 10. (New) The method of claim 2, wherein at least one of the target data and said working key is encrypted according to a default cryptographic algorithm.

Claim 11. (New) The method of claim 2, wherein at least one of the target data and said working key is encrypted according to a user selected cryptographic algorithm.

Claim 12. (New) A method of accessing encrypted target data encapsulated by a secure network packet, comprising:

parsing the secure network packet to provide the encrypted target data and an encrypted working key;

binding together a plurality of key splits to form a cryptographic key;

decrypting, based at least in part on the cryptographic key, the encrypted working key; and

decrypting, based at least in part on the decrypted working key, the encrypted target data to provide decrypted target data;

wherein said plurality of key splits includes a domain key split and a user key split.

Claim 13. (New) The method of claim 12, wherein the secure network packet is accessed at least in part by an integrated circuit.

Claim 14. (New) The method of claim 12, wherein the secure network packet is accessed at least in part by a network interface device.

Claim 15. (New) The decrypted target data and the cryptographic key provided by the method of claim 12.

Claim 16. (New) The method of claim 12, further comprising extracting at least one of said plurality of key splits from a credential store.

Claim 17. (New) The method of claim 12, wherein at least one of said plurality of key splits is a default key split.

Claim 18. (New) The method of claim 12, wherein at least one of said plurality of key splits is selected by a user.

Claim 19. (New) The method of claim 12, wherein at least one of the encrypted target data and the encrypted working key is decrypted according to a default cryptographic algorithm.

Claim 20. (New) The method of claim 12, wherein at least one of the encrypted target data and the encrypted working key is decrypted according to a user selected cryptographic algorithm.